T·D

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/037,267	01/02/2002	Tom Howard	10011529-1	6181

7590 06/22/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
SZYMANSKI, THOMAS M	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 06/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/037,267
Filing Date: January 02, 2002
Appellant(s): HOWARD ET AL.

Michael A. Paparas
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 04/06/2006 appealing from the Office action mailed 01/13/2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5,987,609	Hasebe	11-1999
2002/0004905	DAVIS ET AL	1-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-7, 9, and 11-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hasebe U.S. Patent No. 5,987,609, in view of Davis et al United States Patent Application Publication No. 2002/0004905, and further in view of Barrus et al U.S. Publication No. 2001/0045884

Hasebe has implemented a system that provides for securing the device while running but fails to teach checking the integrity of the system prior to booting for identification of a tampered system.

Davis et al provides for a system within which the integrity of the system is checked for security purposes prior to booting the system (Davis et al paragraph 0018)

Within any system containing data or sensitive access to a system strong security functionality is always desirable to prevent unauthorized acquisition and use of the device and its contents. (Davis et al pg 1 paragraphs 0004-0009)

It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the system of Davis et al with that of Hasebe for the improved security functionality that is obtained from preventing access to the system while it is not connected to the network by the implementation of the integrity checking of the firmware within the system. The Davis et al system when implemented with Hasebe would check the firmware which within the implementation of Hasebe et al

consists of all that is necessary for the operation of the system which is all of that which is contained on ROM and RAM (Hasebe Fig 3, 12 and 13)

Hasebe and Davis have provided a system that provides for storing information in non-volatile memory, but does not explicitly state that the memory is Flash Memory.

Barrus et al provides for a system within which a security protocol is implemented with Flash memory (pg. 2 paragraph 0016).

It is desirable within a security system to be able to implement proactive steps for purposes of improved security, it is especially advantageous to be able to obtain any information as to the possession and or location of such a device when it is in an unauthorized state.

It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the system of Barrus et al with that of the Hasebe/Davis combination. The combination of these two systems forms a better system with improved security measures and thus greater data integrity.

Regarding Claim 1: A device for preventing unauthorized use (Hasebe Col 5 lines 56-67 Col 6 lines 1-67)

Processor (Hasebe Col 4 lines 47-48)

Wireless communication subsystem (Hasebe Col 4 lines 37-46)

Security protocol operable to prevent execution of software upon receiving a message (Hasebe Col 3 lines 21-37, Col 6 lines 44-55 Fig 6) As provided for by Hasebe the security process as implemented allows for prevention of the execution of software by only displaying that which has been selected by the user in fig 6 and not the execution

of any phone functions as such preventing execution of software by the implemented security protocol.

BIOS - The combined system teaches a BIOS as is shown within the background and specification of Davis and furthermore a BIOS that is operable to be verified before being completely loaded as stated within the present invention. In the case of this combination the BIOS itself is inclusive to a security protocol as the software is responsible for access and loading of the system (Davis Paragraphs 4-10) and as stated contains built in security methods lending itself to be understood as a security protocol by the broadest reasonable interpretation of the applicant's claim.

Regarding Claim 2-3: Non-volatile memory for storing information to indicate software is not permitted for execution (Hasebe Col 4 line 45 – Col 6 line 65) As the combination teaches the use of non-volatile flash memory is used for what would have been previously stored on ROM and RAM for the advantages outlined by Barrus. (Barrus paragraphs 4-7, and 16-20)

Regarding Claim 4: Preventing access to user data (Hasebe Fig 6, Col 6 lines 32-59) Hasebe describes several forms of preventing access to the data, one being locking the system and another being deletion of files upon recognition of the device being compromised.

Regarding Claim 5: Protocol causes application to exit if message received while running (Hasebe Col 5 lines 65-67, Col 6 lines 1-7, 23-67) The functionality of the system requires that the program exit while running as that is the manner in which it

must operate. Since the system must be on to receive messages in order to function it must then exit the running normal state in order to implement the selected security level.

Regarding Claim 6: A display for presenting an unauthorized message (Hasebe Fig 3 part 17, Col 6 lines 49-55)

Regarding Claim 7: Implementation within an operating system (Hasebe Fig 3, Col 5 lines 56-67 Col 6 lines 1-67) The system must have an operating system as it would otherwise not function. The security protocol must be implemented within the operating system as it is part of the system and wouldn't have functionality independently. As it can be seen from Fig 3 part 12 the system software is contained together as separate modules reliant upon the operating system.

Claims 9, 11-15 and 16-19 are a method and system implementation of claims 1-7; therefore, claims 9, 11-15 and 16-19 are rejected on the same grounds as presented above.

(10) Response to Argument

A. Davis teaches checking the integrity of a system (of software) before booting, Hasebe teaches a system for disabling a device when not in possession of the rightful owner. The combination of these two systems teaches a system for remotely securing/locking a wireless device wherein the integrity of the system is checked prior to booting any applications. The bios implementation of Davis decides whether or not the system is booted and hence if any application is able to run (Davis paragraph 10, 32-33, Figs 6a,b). A BIOS as understood is a basic operating system that is necessary for any further applications to run on the system (i.e. an OS such as windows and any further

user applications associated with the OS). A BIOS is contained on a device such as a non-volatile memory as described by Davis (fig 5 part 515 paragraphs 30). As seen from Fig 3 of Hasebe the security program is contained on ROM (Col 4 lines 49-55, Col 6 lines 60-67, Fig 3 part 12), which from the implementation of ROM within DAVIS (paragraph 30) is non-volatile ROM that is subject to tampering. Thus when the security protocol of Hasebe is included within the BIOS level implementation of the Davis system a BIOS (Davis Fig 5) as indicated within claim 1 wherein the BIOS is operable to boot the device, verify the integrity (Davis paragraph 23) of said security protocol process before completing boot operations is provided.

The applicant has argued that the authentication process of Davis is separate from the bios and thus cannot be construed as the same entity, however, the two processes are operatively connected within the same device/chip (Davis Fig 5, paragraph 23) and reliant upon each other for operation, since the cryptographic process starts the boot cycle and must authenticate before the BIOS is permitted to run; thus the checking of the protocol, which herein is the BIOS and related systems of Hasebe as contained on ROM and parameterized in RAM (Hasebe Fig 3 parts 13, 23, 24) is performed by this process that is dependent upon the BIOS and therefore considered operatively connected and part of the same system and process of booting.

B. With respect to applicant's argument against claim 2 that hasebe teaches the use of RAM, in combination with the systems of Davis (Davis paragraph 30, Fig 5) and Barrus (Barrus paragraph 16) this system uses Flash memory, as the system of Barrus utilizes flash for all program functions. Additionally, as taught by the combination the

BIOS (Davis paragraph 23, 30) is contained within ROM, similar to that of the security protocol of Hasebe (Fig 3) and settings, which are contained in RAM, wherein from the teachings of the combination these stores are combined as the same. The system of Hasebe teaches storing settings of the security program in RAM, however, RAM is volatile memory and does not retain information with a loss of power, therefore, the combination teaches storing such features in non-volatile memory (Davis paragraph 30, Barrus paragraph 16).

C. The applicant has argued that the system does not teach displaying a message that the rightful user is in possession of the device and points to the described screen lock functionality, however, within the same sighted passage Hasebe discloses an owner indication option that when the device is not in possession of the rightful owner the system displays the owners name and address (Hasebe Fig 6, 12, Col 6 lines 44-46, 49-51, Col 10 lines 20-22), a message that indicates the current user is not the rightful user is thus indicated by displaying the rightful owner's information.

D. Regarding the applicant's argument concerning the rejection not teaching the protocol being implemented in an operating system. As disclosed the system teaches that the BIOS must be loaded prior to operation (Davis paragraph 10). A BIOS in the context of this rejection is considered to be a basic operating system. The security program is operative to run once the system has been authenticated as described by Davis, thus being implemented in the BIOS to prevent unauthorized use (Hasebe Col 2 lines 26-36 Fig 10).

E. Regarding writing information in non-volatile memory indicating that a user is not in rightful possession of the device, the examiner directs attention to the above argument B regarding the teaching of the combination wherein Barrus (paragraph 16) provides security parameters being stored in non-volatile memory as does Davis (paragraph 30, Fig 5). As to storing the message it can be seen from Hasebe Fig 3 part 23 that incoming messages are stored (Col 4 lines 53-65, Col 5 line 65 – Col 6 line 3), and by the teachings of the rejection are stored in non-volatile memory.

F. Regarding the applicant's assertions against claim 13 that displaying a message that the current user is not in rightful possession of the device isn't taught, attention is directed to the above argument C, wherein Hasebe teaches displaying an owner indication (Fig 12, Col 6 lines 44-46, 49-51, Col 10 lines 20-22).

G. In response to the argument concerning the security protocol not running in the operating system attention is directed to D above. Additionally, the applicant has asserted that running on top of and running within the operating system are distinguishable, but the applicant has provided no support to differentiate such a teaching either expressly or implied within the specification and has only alleged the difference. Thus the examiner asserts that as taught the security protocol of Hasebe running with the BIOS operating system teaches a "security protocol process is implemented in an operating system".

H. Regarding the applicant's argument against claim 19 attention is directed to element C above, wherein Hasebe teaches displaying an owner indication (Hasebe Fig 12, Col 6 lines 44-46, 49-51, Col 10 lines 20-22).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

TMS, 6/19/2006 TMS

Conferees:

Matthew Smithers

Gilberto Barron

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Matthew B. Smithers
Patent Examiner
Art Unit 2137